Title: (U) Meeting with [redacted] regarding Blackbyte Ransomware attack
Re: [redacted] 09/27/2021

b3
b6
b7C
b7E

meeting with the [redacted] the Department of Homeland Security and the FBI [redacted] confirmed that a [redacted] network had been infected with Blackbyte Ransomware. The IT personnel that responded to the incident isolated the network and immediately began to work on remediation. All of the infected devices were wiped and were restored from backups. No evidence is available for recovery. No contact was made with the attackers. No ransom was paid. The network has been restored. Following the meeting, attempts to contact [redacted] were unsuccessful.

b6
b7C

♦♦

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) Meeting with [redacted] regarding Blackbyte Ransomware attack **Date:** 09/27/2021 b6 b7C

From: JACKSONVILLE
JK-11 CYBER
Contact: [redacted] b6 b7C b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) INVESTIGATIONS - ZERO FILE b3 b7E

Synopsis: (U) Meeting with [redacted] regarding Blackbyte Ransomware attack b6 b7C

Details:

On September 24, 2021, [redacted] held a virtual meeting with the [redacted] the Department of Homeland Security, FBI TFO [redacted] FBI TFO [redacted] and FBI SA [redacted] advised the following: b6 b7C

The subjects who conduced the Blackbyte Ransomware attack may have exfiltrated data from the [redacted] network. There has been no "proof of life" or hard evidence to support any claims that data was exfiltrated from the network. The ransom note received on 9/19/21 by the [redacted] that demanded a ransom for the compromised data or the data would be publicly posted in 4 days. Forensic images were taken of the backups used to restore the compromised network and an initial analysis of those images show that the network may have been compromised as early as August 19, 2021. Any further evidence collected to include forensic images will be shared with law enforcement. b6 b7C

This meeting was a follow up to the [redacted] captured below. It should be noted that SA [redacted] has made multiple attempts to contact the [redacted] and the [redacted] without success. b6 b7C b7E

Summary of [redacted] b7E

September 19, 2021, SA [redacted] received notification via email regarding a Ransomware attack on the [redacted] network. Multiple attempts to reach the [redacted] were unsuccessful. On 9/20/21, the [redacted] held a virtual b6 b7C